Core Services for Compliant and Trustworthy Data Marketplaces: the EU UPCAST Project

Soulmaz Gheisari[1], Christopher Maidens[1], Semih Yumusak[1], Jaime Osvaldo Salas[1], Paolo Pareti[1], George Giamouridis[1], Miao Hu[1], Adeel Aslam[1], Bijay Prasad Jaysawal[1], Luis-Daniel Ibáñez[1], George Konstantinidis[1] and Dumitru Roman[2]

[1]*Department of Electronics and Computer Science, University of Southampton, Southampton, UK*
[2]*SINTEF, Oslo, Norway*

Abstract

Compliance and trustworthiness are critical to the success of modern data marketplaces, where sensitive information is exchanged across organisational and jurisdictional boundaries. The UPCAST project addresses these challenges through a modular, plugin-based architecture that integrates privacy-preserving consent management, dynamic policy enforcement, and negotiation services. This paper presents the design and interaction of UPCAST's core services, focusing on the bidirectional integration of Consent Management and Negotiation to ensure that agreements are legally sound, policy-compliant, and transparent to all stakeholders. By embedding compliance verification and trust assessment into the negotiation lifecycle, UPCAST moves beyond post-hoc auditing towards real-time, context-aware enforcement. The resulting architecture enables marketplaces that are adaptable to evolving regulatory requirements, interoperable across sectors, and capable of supporting secure, transparent, and mutually beneficial data transactions.

Keywords

Consent management, Core services, Data marketplace, Negotiation manager, Policy editor, Privacy manager, Trust and reputation

1. Introduction

The *UPCAST* project[1] (Unified Platform for Connected, Compliant, and Trustworthy Data Spaces) is an EU-funded initiative aimed at delivering an open, modular, and extensible platform for designing and deploying next-generation data marketplaces. Its primary goal is to enable secure, compliant, and transparent data sharing among heterogeneous stakeholders across domains such as mobility, energy, and health, while respecting applicable regulations such as the General Data Protection Regulation (GDPR) [1] and emerging European data governance legislation, including the Data Governance Act [2], the Data Act [3], and the Digital Markets Act [4].

UPCAST adopts a *plugin-based architecture* to allow its components to be flexibly deployed, extended, or replaced depending on marketplace requirements. In this architecture, **Core Services** provide functionalities such as authentication, policy management, consent handling, negotiation, trust assessment, contract generation, monitoring, and contextual awareness (*State of the World*). These are complemented by **Client Services** for user interaction (e.g., Privacy Manager, Negotiation Manager, Data-asset Submission Manager) and **Specialised Services** for specific value-added capabilities (e.g., ontology-based policy authoring, workflow handling, natural language support). By separating these

RuleML+RR'25: Companion Proceedings of the 9th International Joint Conference on Rules and Reasoning, September 22–24, 2025, İstanbul, Türkİye

s.gheisari@soton.ac.uk (S. Gheisari); C.Maidens@soton.ac.uk (C. Maidens); semih.yumusak@soton.ac.uk (S. Yumusak); j.o.salas@soton.ac.uk (J. O. Salas); P.Pareti@soton.ac.uk (P. Pareti); g.giamouridis@soton.ac.uk (G. Giamouridis); Miao.Hu@soton.ac.uk (M. Hu); A.Aslam@soton.ac.uk (A. Aslam); B.P.Jaysawal@soton.ac.uk (B. P. Jaysawal); l.d.ibanez@soton.ac.uk (L. Ibáñez); g.konstantinidis@soton.ac.uk (G. Konstantinidis); dumitru.roman@sintef.no (D. Roman)
0000-0001-8974-2841 (S. Gheisari); 0000-0002-4385-7202 (C. Maidens); 0000-0002-8878-4991 (S. Yumusak); 0000-0002-9353-8955 (J. O. Salas); 0000-0002-2502-0011 (P. Pareti); 0009-0009-8353-1862 (G. Giamouridis); 0000-0001-9055-563X (M. Hu); 0000-0002-5491-2967 (A. Aslam); 0000-0001-6958-0347 (B. P. Jaysawal); 0000-0001-6993-0001 (L. Ibáñez); 0000-0002-3962-9303 (G. Konstantinidis); 0000-0001-6397-3705 (D. Roman)

[1]https://www.upcast-project.eu/

functionalities into modular services, UPCAST facilitates interoperability and promotes the creation of data marketplaces that can adapt to evolving business models and regulatory landscapes. Beyond its conceptual design, UPCAST is implemented in collaboration with industry leaders and operates in concrete marketplace environments, including telecommunications-focused marketplaces led by Nokia [2] and cross-sectoral platforms provided by Dawex [3]. These deployments demonstrate the framework's applicability across domains with distinct regulatory, technical, and business constraints, and provide a valuable proving ground for the compliance and trust mechanisms described in this paper.

The conceptual and architectural foundations of UPCAST have been discussed in [5], which presents a generic modular design pattern for data marketplaces, identifies a set of reusable marketplace *plugins*, and demonstrates how such an approach supports flexibility, composability, and compliance. That work emphasises the importance of a plugin-oriented perspective for ensuring that marketplaces can be incrementally extended and maintained without requiring extensive redesign.

In this paper, we build upon those architectural principles and focus specifically on the **Core Services for Compliant and Trustworthy Data Marketplaces** within UPCAST, with particular emphasis on *privacy-preserving consent management* and *negotiation workflows*. We present the updated UPCAST architecture highlighting how these services interact bidirectionally to ensure that all negotiated agreements are legally sound, policy-compliant, and transparent to stakeholders. Our contribution is twofold: (i) to detail the design and integration of Privacy and Negotiation services in the UPCAST framework, and (ii) to demonstrate how these components collectively operationalise compliance and trust throughout the data marketplace transaction lifecycle. The remainder of this paper is structured as follows. Section 2 introduces the UPCAST Core Services for compliance and trust, including Section 2.1 by a detailed description of the privacy services and their integration into marketplace workflows and Section 2.2 focuses on the automated negotiation capabilities. Section 3 reviews the state of the art in data marketplace architectures. Finally Section 4 concludes the paper with key findings and outlines directions for future work.

2. UPCAST Core Services for Compliance and Trust

We organise the UPCAST Core Services for compliance and trust into three main categories of services: **Policy Services**, **End-to-End Services**, and **Support Services**. Each category is implemented as a set of independently deployable *services*, enabling flexible composition and seamless integration into diverse marketplace deployments. Figure 1 presents the updated UPCAST Core Services architecture, highlighting the interactions that underpin compliance and trust in the marketplace transaction lifecycle.

Policy Services in UPCAST provide the foundation for expressing and enforcing data usage rules. The **UPCAST Policy Editor** allows stakeholders to create and maintain machine-readable policies using languages such as the *Open Digital Rights Language* (ODRL) [6] and the *Data Privacy Vocabulary* (DPV) [7]. Specialised services such as the **ODRL Editor** and **Ontology Editor** support fine-grained control over permissible actions, obligations, and constraints. All validated policies are stored in a policy data store, which serves as the authoritative source for compliance verification across the marketplace.

Note that Policy Services are not isolated; they interface directly with Consent Management to ensure that end-user permissions are aligned with contractual and regulatory requirements.

End-to-End Services implement the primary operational workflows of the marketplace, integrating compliance checks into every transaction stage. **UPCAST Consent Management** service is responsible for capturing, storing, and validating consent in accordance with the defined policies. It maintains a bidirectional link with the **UPCAST Negotiation Service**, to verify that proposed terms respect the current consent state, prior to negotiation. And after negotiation, it records any updated consent derived from contractual agreements. The Negotiation Service also coordinates with other operational services. **Trust and Reputation Management** provides quantitative trust scores to guide negotiation strategies. **WorkFlow Editor** supports users to describe their intended sequence of operations.

[2] https://www.nokia.com/es_int/nokia-en-espana/
[3] https://www.dawex.com/en/

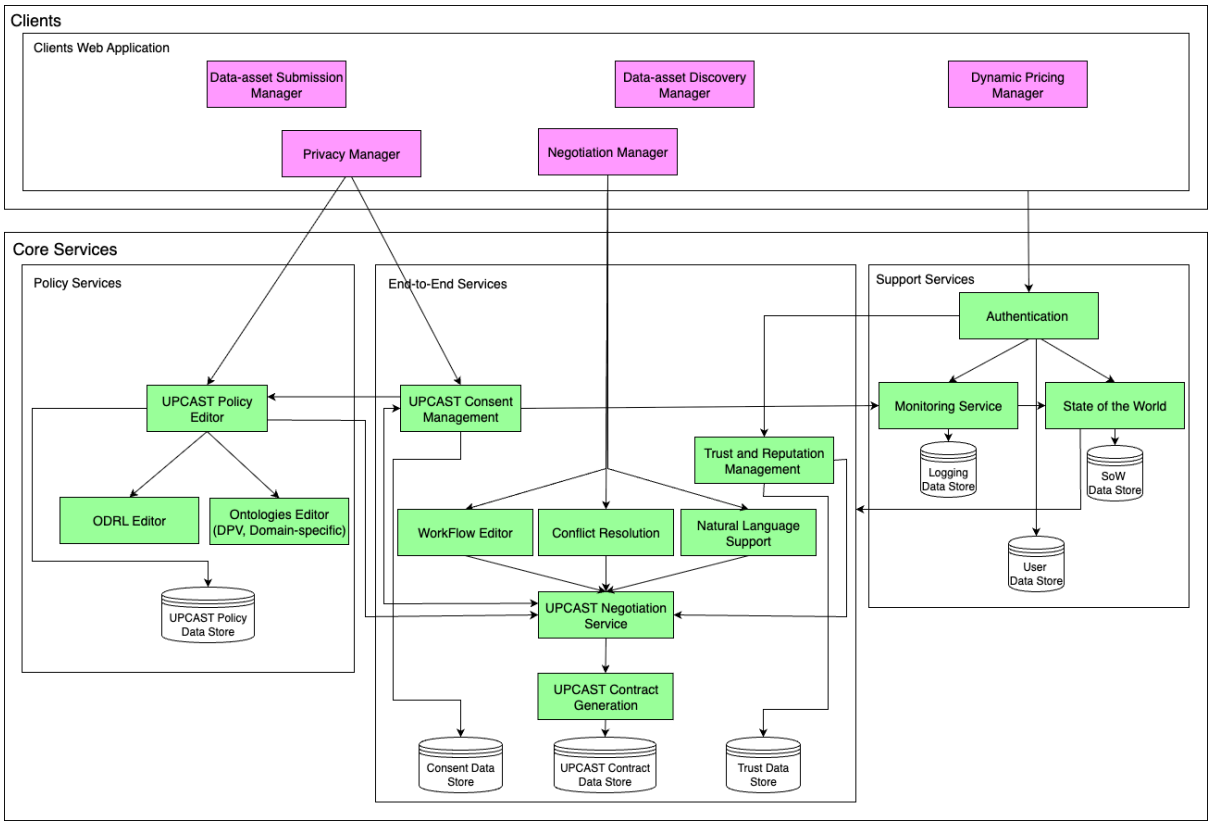

Figure 1: UPCAST Core Services for Compliance and Trust, showing Privacy and Negotiation integration.

Conflict Resolution proposes compliant alternatives when terms clash with policies or consents. **Natural Language Support** generates human-readable explanations of contractual clauses. Successful negotiations are passed to the **Contract Generation** service, producing both machine-executable and human-readable agreements stored in a contract repository.

Support Services provide cross-cutting functionality to ensure that compliance and trust are maintained across all marketplace operations. The **Monitoring Service** continuously logs consent events, policy enforcement actions, and contract executions. The **State of the World** service aggregates contextual information such as jurisdiction-specific rules, market conditions, or external compliance alerts, which can directly influence negotiation outcomes. The **Authentication** service enforces access control to ensure that only authorised actors can participate in policy editing, consent management, or negotiation.

The integration of these three service categories within the UPCAST plugin-based architecture ensures that compliance is embedded into the operational fabric of the marketplace, rather than being an external or manual verification process. In the following, we focus on two of the most critical capabilities for achieving both compliance and trust: *privacy-preserving services* and *negotiation services*.

2.1. Privacy-Preserving Services in UPCAST

Privacy protection in UPCAST is implemented as an integrated set of services that span the client, policy, and operational layers of the architecture. Rather than treating privacy as a static compliance requirement, UPCAST embeds it into the transaction lifecycle through dynamic consent management, continuous monitoring, and contextual adaptation.

The **Privacy Manager at the Client Layer** operates at the client-facing layer, enabling data subjects and data providers to configure and communicate their privacy preferences in a structured, machine-interpretable format. These preferences can include various issues such as, the specific purposes for

which data may be used, applicable usage constraints (e.g., time limits), and revocation or modification rules for previously granted permissions.

The Privacy Manager transmits these preferences to the consent management service for validation against active policies.

The **UPCAST Consent Management** service works as the authoritative system of record for all consent-related information. It interacts bidirectionally with the UPCAST Negotiation Service to: (1) Verify that proposed terms in an ongoing negotiation align with the current consent state. (2) Update the consent data store once a contract is finalised, ensuring that downstream enforcement mechanisms have an up-to-date reference.

Consent Management also interfaces with the UPCAST Policy Editor to ensure that consents are consistent with regulatory requirements expressed in marketplace policies.

The **Monitoring and Auditability** ensures full traceability of privacy-related actions and provides verifiable evidence for regulatory audits. All consent events—grants, revocations, expirations, and violations—are sent from Consent Management to the Monitoring Service as structured audit logs.

The **State of the World** enhances privacy decision-making by driving contextual constraints into the consent validation process. For example, it can provide updates on jurisdiction-specific regulations, contractual obligations inherited from upstream data sources, or newly published compliance guidelines. This allows privacy enforcement to adapt dynamically to changing conditions, reducing the risk of inadvertent policy breaches.

By combining these capabilities, UPCAST operationalises *privacy-by-design* principles as the following:

- Privacy constraints are explicitly captured at the point of data onboarding or transaction initiation.
- Enforcement is continuous and context-aware, rather than periodic or reactive.
- All actions are logged for transparency and accountability.

This design ensures that privacy is not merely a contractual clause but an actively enforced property of the marketplace's operation.

2.2. Negotiation-Support Services in UPCAST

The UPCAST Negotiation Service [4] is responsible for managing the offer–counteroffer process between marketplace participants, ensuring that contractual terms are both economically optimal and compliant with applicable policies and user consents. In the UPCAST architecture, negotiation is not a standalone process but is tightly integrated with other compliance-critical services.

WorkFlow Editor provides a service to define acceptable workflow patterns from data provider side and intended workflow from data consumer side. Upon receiving a request to access a data source, negotiation begins with compliance pre-check, it queries the **Consent Management** plugin to determine whether the proposed terms in the align with existing consent records. If the terms of negotiation violate an active consent constraint or or the intended workflow breaches the provider's admitted patterns the negotiation service triggers the **Conflict Resolution** service to propose compliant alternatives. Negotiation continues by offer and counteroffer back and forth. Once an agreement is reached, the updated terms are written back to a consent data store to ensure downstream enforcement. This bidirectional interaction ensures that no agreement can bypass established privacy constraints.

To enhance transparency, the **Natural Language Support** service generates human-readable summaries of proposed contract terms and policy constraints. This ensures that all parties, regardless of technical expertise, can fully understand the terms being negotiated.

When negotiation concludes, the **Contract Generation** plugin produces both *Human-readable agreements* for legal review and signature and *Machine-executable agreements* for automated enforcement. Contracts are stored in a contract repository and linked to their corresponding consent and policy records, enabling continuous compliance monitoring.

[4]UPCAST negotiation protocol extends the Contract Negotiation Protocol (CNP) defined by the International-Data-Spaces-Association (IDSA) [8].

The **Trust and Reputation Management** plugin maintains dynamic trust scores for all marketplace participants, informed by historical contract fulfilment rates, recorded policy violations, and peer-provided ratings. These trust metrics influence negotiation strategies, allowing the Negotiation Service to prioritise agreements with high-reputation entities and to adjust contract terms for lower-reputation parties.

3. Background and Related Work

The development of data marketplaces has accelerated in recent years, driven by the need to enable controlled and value-generating data sharing across organisational and sectoral boundaries. Architectures for such marketplaces vary from centralised platforms to fully decentralised, peer-to-peer systems, and hybrids that combine elements of both. Several prominent European initiatives have sought to provide reference architectures and governance frameworks for trusted data sharing.

The **International Data Spaces** (IDS) [9] framework introduces the concept of *connectors* to enforce data usage policies and contractual obligations, with a strong emphasis on interoperability and data sovereignty. Similarly, **Gaia-X** [10] defines a federated infrastructure for data exchange, focusing on trust through certification, identity management, and standardised service descriptions. The **i3-MARKET** project [11] has explored decentralised data marketplaces with blockchain-based trust anchors. While each of these initiatives addresses critical aspects of interoperability and compliance, their architectural models tend to be more monolithic or require substantial integration effort when adapting to specific sectoral needs.

The **UPCAST** project advances this state of the art by adopting a *plugin-based architecture* [5], where *Core Services* and *Plugins* can be independently deployed, extended, and replaced. This design philosophy supports rapid adaptation to new regulatory requirements, emerging data usage scenarios, and evolving market demands. In UPCAST, plugins encapsulate discrete marketplace capabilities—such as ontology-driven policy authoring, consent management, negotiation, trust and reputation assessment, and contract generation—each of which can be integrated into different deployment contexts without altering the core architecture.

This modularity enables UPCAST to balance **compliance**, **trustworthiness**, and **interoperability** while avoiding the rigidity often found in monolithic designs. Moreover, the explicit separation between *Policy Services*, *End-to-End Services*, and *Support Services* in UPCAST allows stakeholders to compose marketplace instances that are tailored to both their operational and compliance needs.

In this paper, we leverage this modular architecture to examine, in depth, two key capabilities essential to compliant and trustworthy data exchange: **privacy-preserving consent management** and **automated negotiation services**. By analysing their integration and interaction within the UPCAST framework, we aim to demonstrate how compliance can be operationalised as a *first-class property* of the marketplace transaction lifecycle, rather than a post-hoc verification step.

4. Conclusion

We present the design of UPCAST's core services for enabling compliant and trustworthy data marketplaces, focusing on the integration of privacy-preserving consent management and negotiation process. Through its plugin-based architecture, UPCAST embeds compliance into the operational fabric of the marketplace, ensuring that agreements are both legally sound and aligned with user-defined constraints.

By maintaining a bidirectional link between Consent Management and the Negotiation Service, the architecture ensures that compliance is validated in real time, rather than as a post-processing step. The inclusion of Trust and Reputation Management, Conflict Resolution, and Natural Language Support further strengthens the reliability and transparency of negotiated agreements.

Future research and development will extend UPCAST's capabilities in several directions such as: (1) Expanding UPCAST Policy Editor to cover domain-specific regulatory requirements and emerging AI

governance standards. (2) Modeling the negotiation process as a strategic game, and automating the whole negotiation process.

By pursuing these enhancements, UPCAST aims to set a benchmark for compliance and trust in data marketplaces, offering a flexible, modular, and future-proof foundation for secure data exchange across diverse sectors.

Acknowledgments

This work was funded by the UKRI Horizon Europe guarantee funding scheme for the Horizon Europe projects UPCAST (10.3030/101093216).

Declaration on Generative AI

The authors declare that ChatGPT were used in the preparation of this manuscript to improve language clarity and grammar in certain sections under the authors' direction."

References

[1] European Union, Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (general data protection regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj, 2016. Accessed: 2025-07-30.

[2] European Parliament and Council of the European Union, Regulation (EU) 2022/868 of the European Parliament and of the Council on European data governance (Data Governance Act), https://eur-lex.europa.eu/eli/reg/2022/868/oj, 2022. Official Journal of the European Union, L 152, 3.6.2022.

[3] European Parliament and Council of the European Union, Regulation (EU) 2023/2854 of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), https://eur-lex.europa.eu/eli/reg/2023/2854/oj, 2023. Official Journal of the European Union, L 2023, 22.12.2023.

[4] European Parliament and Council of the European Union, Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), https://eur-lex.europa.eu/eli/reg/2022/1925/oj, 2022. Official Journal of the European Union, L 265, 12.10.2022.

[5] S. Gheisari, S. Yumusak, J. O. Salas, L.-D. Ibáñez, G. Konstantinidis, D. Roman, Towards modular data marketplaces (2024).

[6] R. Ianella, Open digital rights language (odrl), Open Content Licensing: Cultivating the Creative Commons (2007).

[7] H. J. Pandit, B. Esteves, G. P. Krog, P. Ryan, D. Golpayegani, J. Flake, Data privacy vocabulary (dpv)–version 2.0, in: International Semantic Web Conference, Springer, 2024, pp. 171–193.

[8] Contract Negotiation Protocol (CNP), International Data Spaces Association, 2024. URL: https://docs.internationaldataspaces.org/ids-knowledgebase/dataspace-protocol/contract-negotiation/contract.negotiation.protocol, part of the Dataspace Protocol, version 2024-1.

[9] International Data Spaces Association, International Data Spaces Reference Architecture Model, https://internationaldataspaces.org/use/reference-architecture/, 2023. Version 4.0.

[10] Gaia-X European Association for Data and Cloud AISBL, Gaia-X Architecture Document, https://gaia-x.eu/, 2023. Version 23.10.

[11] i3-MARKET consortium, i3-MARKET: Intelligent, interoperable, integrative and deployable open-source marketplace backplane, European Union Horizon 2020 Project, 2020. URL: https://cordis.europa.eu/project/id/871754, grant Agreement ID: 871754.